Senate Committee on Information Technologies (SCIT)
February 11, 2019
Minutes of the Meeting

These minutes reflect discussion and debate at a meeting of a committee of the University of Minnesota Senate; none of the comments, conclusions or actions reported in these minutes reflect the views of, nor are they binding on, the senate, the administration or the Board of Regents.

[**In these minutes:** Welcome and Introductions; Data Privacy and Technology; Review of Information Security Policy, Procedures, and Appendices]

PRESENT: Geoffrey Ghose (chair), Nancy Carpenter, William Dana, Michelle Driessen, Bernard Gulacheck, Kristin Janke, Jonathan Koffel, Robert Rubinyi, Daniele Sandler, Yoichi Watanabe, Rodney Williams

REGRETS: Al Beitz, John Butler, Santiago Fernandez-Gimenez, Karen Monson, Timothy Nichols, Carlos Soria

ABSENT: Arash Mahnan, Charles Miller, Paul McSpadden

GUESTS: Susan McKinney, director, Records and Information Management, Joe Dufresne, University information security manager, and Barb Montgomery, security analyst, University Information Security Services

1. Welcome and Introductions

Chair Geoffrey Ghose called the meeting to order and noted that today's meeting would be centered around privacy and security policies at the University. He then turned the meeting over to the day's first speaker.

2. Data Privacy and Technology

Susan McKinney, director, Records and Information Management, introduced herself and gave a brief synopsis of her work in the privacy and records management field. She then distributed a handout delineating the University's stance on private versus public information. McKinney noted that there are numerous laws governing privacy at the University, including the Family Educational Rights and Privacy Act of 1974 (FERPA), the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and the Federal Policy for the Protection of Human Subjects (The Common Rule) for research. She added that the Minnesota state law that governs privacy issues at the University is the Minnesota Government Data Practices Act.

McKinney explained that through the Minnesota Government Data Practices Act, the state considers all information to be public, as a starting point, unless there is a specific statute that renders it private. She pointed out the list of employee and student information that is private, according to University policy, followed by a longer list that is considered public information. She added that when the University receives a request for data, it is imperative to give out public data only.

Sometimes the federal and state laws are not in complete alignment, McKinney pointed out, and each may request different levels of access to information such as research. As an example, she said, the federal Freedom of Information Act (FOIA) requires access to more data in research documents than is required at the state level; the University is not able to designate as much unpublished research data as protected by trade secret at the federal level as it can at the state level. McKinney continued that when the University receives a FOIA request, it most often has to do with research, usually is coming from one of the major research agencies, and is most often associated with grant proposals.

McKinney pointed out that because the Minnesota state law states that everything is public, emails, text messages, and anything done on a home computer or personal device *for University work*, is considered public.

At this point, McKinney asked if there were questions.

Robert Rubinyi asked to clarify if University business conducted on *personal devices* was considered public information, and McKinney said it would fall under the Data Practices Act, but whether or not it was public information would depend on the content of the information. Rubinyi then asked if everything a University employee does - with data and communication, even storing data in a file cabinet, for example - would fall under the Data Practices Act, if there were no exemptions in place. McKinney confirmed that Rubinyi was correct, and that when data and information are no longer needed, they should be disposed of. She added that this was true for texts, emails, phone messages and recordings, as well as information and data on paper. Should there be a security breach, for example, there would then be much less material that could be adversely affected, McKinney explained.

Daniela Sanders, concerned about phishing attempts and other scams, asked if it was possible to not have one's email address listed as public information. She said she understood the importance of being reachable by staff and students, but wondered about ways to avoid possible hacking and phishing. McKinney explained that while email addresses are considered public information under the Data Practices Act, that does not mean that they have to be listed; it simply means that if someone *requests* an email address, it has to be given to them. The policy discussion that should be considered, McKinney said, is how does the University want to manage directory information for employees and students. She added that some universities require authentication to access the directory information, so only employees of the institution have access. There are pros and cons to both ways of maintaining the data, said McKinney, and how to protect and store the data is something she hoped the SCIT would continue to discuss and weigh in on.

Bernie Gulachek noted that the discussion about whether or not to keep information behind an authentication "wall" is currently taking place in the Office of the Registrar as well as in the Office of Human Resources. Gulachek added that the challenge is that by law, email addresses are public information, and if asked for them, the University is obliged to provide them. Should the University decide to use authentication, the next decision would be who will provide that information when it is asked for, and what will the process look like, Gulachek explained.

Gulachek and McKinney both noted that while this is a decision that the University needs to have discussions about and consider thoroughly, using authentication will most likely not reduce the amount of phishing that occurs.

Joe Dufresne, University information security manager, University Information Security Services, added that one of the ways information is taken is by "scraping" entire directories to programmatically take every address and spam them. He said the University can make it more difficult for that kind of activity to take place while still having a public directory. Dufresne noted that the University is behind its Big 10 peers in the amount of information that is available to the public; many of them have the information behind a log-in or authentication.

Rubinyi noted that there may be a public policy component at work as well; the University has an outreach function, legislators and community members often need to reach people at the University. He applauded the idea of less scraping and phishing, but thought that putting information behind a firewall might do more harm than good for the institution.

Ghose raised the question of needing his email address to be available for work such as anonymous peer review which is done for journals, for grants, etc., and wondered what are the laws governing keeping that information public? McKinney explained that there is one law that categorically says information either is or is not public. She then went on to describe how many situations are not black and white, but reside in a gray area. The trade secret provision will often be used to look at information being requested, McKinney said, when that information contains unpublished work, licensing, or copyright requirements, in an attempt to keep it private.

She next described situations in which University personnel may be working for another organization, and while they are employed by the University, the work being done on behalf of the other organization could be considered "non-university product," which may allow it to remain private. When doing work or research for another organization, McKinney noted, it is recommended that an employee keep a document management system that keeps the work for the organization separated from University work, along with requesting a separate email from the organization. This may aid in making a stronger argument for keeping the work private, McKinney said, as it is work done not for the University but for the other organization.

McKinney led a robust conversation around the scope of public and private information, University versus non-University product, and the state and federal laws that guide the decisions that are made as to what information must be distributed when requested.

Michelle Driessen then asked about instructor access to useful student data, and the levels of privacy surrounding it. McKinney noted that almost all student data starts out as private.When you start to look at learning analytics, she commented, the important questions are not who can access the information and how is it done, but *what is going to be done with the information*. There are significant management issues surrounding learning analytics and data ethics, and these are topics that are being broadly discussed, not only at the University of Minnesota but at universities nationwide, McKinney said.

Gulachek noted that as systems modernize, more extremely detailed data becomes available. Gulachek then asked how will the University respond to these questions:

- How do we work with learning analytics?
- Who has access to them?
- Who owns them?
- How do we fulfill the requests for the information?

Gulachek listed both pros and cons of using information derived from learning analytics. Learning analytics have the potential to help students succeed in the classroom as well as to assist faculty in refining their pedagogy. On the other hand, he asked, can learning analytics be misused for profiling or other negative outcomes? Gulachek added that the topic is being widely debated throughout higher education, and the University will need to craft and put in place policies that will enable the institution to use the data appropriately in fulfilling its mission.

McKinney reminded everyone that when working with this type of data, if it is anonymized, it becomes public data. Once the data is made public, data brokers will want to use it, and there is no way to stop that, McKinney warned, unless a statute is added to the Data Practices Act. McKinney stressed the importance of remembering this fact in order to avoid unintended consequences, as research and policy planning continue.

William Dana asked if there was a way to return or store his work product with the University, rather than retaining all files himself and deciding which to keep and which to delete. McKinney suggested speaking with the University Libraries regarding the Digital Conservancy and how to manage research project data.

At this point, McKinney finished her presentation and left the meeting.

3. Review of Information Security Policy, Procedures, and Appendices

Gulachek then introduced Joe Dufresne and Barb Montgomery from University Information Security Services to present information on the University's Information Security Policy. Gulacheck briefly described how the Information Security Policy informs data analysts of best practices for securing different types of data.

Dufresne began by noting this review is part of the University's standard review process and that this particular policy was not undergoing any significant changes. The changes consist of identifying gaps, deleting duplicate material, adding language that reflects changes in the law, and adding software development guidelines, Dufresne explained.

A conversation followed about how an individual complies with the data safety requirements within the policies, and the resources that are available at the University to help with compliance. Dufresne explained that it is incumbent upon the University to determine how to safeguard its data. He added that University Information Security Services has a risk assessment process that can be done on information in individual departments where the safety of that department's data and information is in question. He noted that University Information Security Services has different types of security awareness training options, including a 30-minute training on

information security that all new staff and student employees take, and training sessions that can be tailored to team meetings.

Ghose asked a question about how data on iphones, laptops, and mobile devices is protected if, for example, the device is lost or stolen. Dufresne explained that there are usually more protections on a University-issued device than on a personal device, and more extensive controls around devices used in the healthcare unit of the University than other units. He added that there is the ability to encrypt information and do remote wipes, should sensitive data on these devices be compromised.

Ghose then invited discussion about proactive versus reactive responses to potential data breaches. Gulachek began by saying that in the industry of information security, there are both people who get out ahead of problems before they occur, and those who react to the problems. The University has been watching trends in the security field, monitoring compromised accounts, and early on understood that two-factor authentication was something that was necessary to prevent breaches at the University and, therefore, got out ahead of it.

Gulachek described a number of ways that the University is working through policies, recommendations and best practices to create strategic and proactive approaches to data security rather than reactive ones.

Committee members and guests had a robust discussion around the issue of privacy, and what an employer can or should be allowed to install on an employee's phone or device in the name of data security. Dufresne noted that many fewer controls are put on devices in the academic sphere than in the corporate sphere. Gulachek added that the type of industry will, to some extent, determine the amount of and kinds of controls put on information. He stressed that the University is a public entity and therefore all data starts out public, with limited exceptions. Technical controls are then put around those exceptions for security, Gulachek said. The challenge for the University, Gulachek stated, is to find systematic approaches and methodologies for managing risk, while recognizing that risk cannot be eliminated completely.

Seeing no further business, Ghose adjourned the meeting.

Geanette Poole
University Senate Office